CLAIMS

What is claimed is:

1. In a first node of a physical network supporting multiple virtual network connections, a method to dynamically modify configuration data supporting virtual networks, the method comprising:

receiving i) network address information associated with at least one host computer, and ii) a corresponding gateway identifier of a gateway in the physical network;

generating a notification message including the network address information and the corresponding gateway identifier; and

transmitting the notification message to a second node of the physical network enabling the second node to establish a virtual network connection between the second node and the first node on which to forward data messages to the at least one host computer based on the corresponding gateway identifier.

2. A method as in claim 1, wherein generating a notification message further comprises:

generating at least a portion of the notification message in accordance with a distribution protocol utilized by service providers to disseminate routing policy information to customer edge nodes; and

wherein transmitting a notification message includes:

transmitting the network address information and the corresponding gateway identifier as an appendix to the notification message.

3. A method as in claim 2, wherein the distribution protocol is based at least in part on an interautonomous system routing protocol and the virtual network connection between the second node and the first node is a virtual private network connection overlaid on the physical network, one end of the virtual private

network connection terminating at the gateway identified by the corresponding gateway identifier.

4. A method as in claim 1 further comprising:

transmitting routing policy attribute information in addition to the network address information and corresponding gateway identifier to the second node to more particularly define a policy for routing the data messages on a corresponding virtual network connection through the gateway to the at least one host computer.

5. A method as in claim 1, wherein the first and the second nodes are part of a network that does not inherently support encryption services and configuration data at the second node at least partially supports encryption of data messages forwarded to the at least one host computer through the gateway identified by the corresponding gateway identifier.

6. A method as in claim 1, wherein transmitting the network address and identifier includes:

delivering the notification message including the network address and corresponding gateway identifier to multiple customer edge nodes of the physical network, each customer edge node updating its corresponding configuration data for establishing private networks between the customer edge nodes based on the network address and corresponding gateway identifier.

7. A method as in claim 1, wherein the first and second nodes are customer edge nodes in a network and the network supports virtual private networks terminating at the customer edge nodes.

8. A method as in claim 1, wherein the network address information identifies a single host computer.

9. A method as in claim 1, wherein the network address information identifies a range of host computers that are part of a network coupled to the first node.

10. A method as in claim 1, wherein the corresponding gateway identifier is an IPsec identity associated with the at least one host computer.

11. A computer system at a first node of a physical network that at least partially supports a virtual network connection, the computer system comprising:

a processor;

a memory unit that stores instructions associated with an application executed by the processor;

a communication interface that supports communication with other nodes of the physical network; and

an interconnect coupling the processor, the memory unit, and the communication interface, enabling the computer system to execute the application and perform operations of:

receiving i) network address information associated with at least one host computer, and ii) a corresponding gateway identifier of a gateway in the physical network;

generating a notification message including the network address information and the corresponding gateway identifier; and

transmitting the notification message to a second node of the physical network enabling the second node to establish a virtual network connection between the second node and the first node on which to forward data messages to the at least one host computer based on the corresponding gateway identifier.

12. A computer system as in claim 11 that, when generating a notification message and respectively transmitting a notification message, further performs operations of:

generating at least a portion of the notification message in accordance with a distribution protocol utilized by service providers to disseminate routing policy information to customer edge nodes; and

transmitting the network address information and the corresponding gateway identifier as an appendix to the notification message.

13. A computer system as in claim 12, wherein the distribution protocol is based at least in part on an interautonomous system routing protocol and the virtual network connection between the second node and the first node is a virtual private network connection overlaid on the physical network, one end of the virtual private network connection terminating at the gateway identified by the corresponding gateway identifier.

14. A computer system as in claim 11 that further performs an operation of:

transmitting routing policy attribute information in addition to the network address information and corresponding gateway identifier to the second node to more particularly define a policy for routing the data messages on a corresponding virtual network connection through the gateway to the at least one host computer.

15. A computer system as in claim 11, wherein the first and the second nodes are part of a network that does not inherently support encryption services and configuration data at the second node at least partially supports encryption of data messages forwarded to at least one host computer through the gateway identified by the corresponding gateway identifier.

16. A computer system as in claim 11 that, when transmitting the network address and identifier, further performs operations of :

delivering the notification message including the network address and corresponding gateway identifier to multiple customer edge nodes of the physical network, each customer edge node updating its corresponding configuration data

for establishing private networks between the customer edge nodes based on the network address and corresponding gateway identifier.

17. A computer system as in claim 11, wherein the first and second nodes are customer edge nodes in a network configured according to Request For Comment 2547 and the network supports virtual private networks terminating at the customer edge nodes.

18. A computer system as in claim 11, wherein the network address information identifies a single host computer.

19. A computer system as in claim 11, wherein the network address information identifies a range of host computers that are part of a network coupled to the first node.

20. A computer system as in claim 11, wherein the corresponding gateway identifier is a network address of the at least one host computer.

21. In a receiving node of a physical network supporting multiple virtual network connections, a method to dynamically modify configuration data associated with at least one of the multiple virtual network connections, the method comprising:

receiving a notification message from a sending node of the physical network, the notification message including network address information and a corresponding gateway identifier of a gateway of the physical network; and

based on contents of the notification message, modifying a map at the receiving node to include the network address information and configuration data identifying at least part of a virtual network connection between the receiving node and the sending node on which to forward data messages through the gateway to a destination node.

22. A method as in claim 21 further comprising:

upon forwarding data messages through the receiving node, utilizing the map to identify on which virtual network to forward the data messages through the gateway to the destination node.

23. A method as in claim 21 further comprising:

at the receiving node including the map, receiving a data message to be forwarded based on a corresponding destination address;

comparing the destination address and a source address of the data message to network address information stored in the map;

identifying, based on the destination address, how to transmit the data message to the destination node based on a corresponding virtual network connection specified in the map.

24. A method as in claim 23 further comprising:

in response to identifying that the destination address of the data message matches network address information in the map, establishing the corresponding virtual network connection specified in the map on which to transmit the data message to the destination node.

25. A method as in claim 24, wherein establishing a virtual network connection includes establishing a virtual private network connection between the receiving node and sending node based on IKE (Internet Key Exchange) protocol and Ipsec (Internet Protocol Security).

26. A method as in claim 23 further comprising:

in response to identifying that the destination address of the data message matches network address information in the map, identifying whether a corresponding virtual network connection specified in the map has been

established and, if so, transmitting the data message on the established virtual network connection to the destination node.

27. A method as in claim 21, wherein the network address information identifies a single host computer.

28. A method as in claim 21, wherein the network address information identifies a range of host computers that are part of a network coupled to the first node.

29. A method as in claim 21, wherein the corresponding gateway identifier is an IPsec identity associated with the at least one host computer.

30. A method as in claim 21, wherein the gateway is located in the sending node.

31. A computer system at a receiving node of a physical network that at least partially supports a virtual network connection, the computer system comprising:

a processor;

a memory unit that stores instructions associated with an application executed by the processor;

a communication interface that supports communication with other nodes of the physical network; and

an interconnect coupling the processor, the memory unit, and the communication interface, enabling the computer system to execute the application and perform operations of:

receiving a notification message from a sending node of the physical network, the notification message including network address information and a corresponding gateway identifier of a gateway of the physical network; and

based on contents of the notification message, modifying a map at the receiving node to include the network address information and

configuration data identifying at least part of a virtual network connection between the receiving node and the sending node on which to forward data messages through the gateway to a destination node.

32. A computer system as in claim 31 that further performs an operation of:

upon forwarding data messages through the receiving node, utilizing the map to identify on which virtual network to forward the data messages through the gateway to the destination node.

33. A computer system as in claim 31 that further performs operations of :

at the receiving node including the map, receiving a data message to be forwarded based on a corresponding destination address;

comparing the destination address and a source address of the data message to network address information stored in the map;

identifying, based on the destination address, how to transmit the data message to the destination node based on a corresponding virtual network connection specified in the map.

34. A computer system as in claim 33 that further performs operations of:

in response to identifying that the destination address of the data message matches network address information in the map, establishing the corresponding virtual network connection specified in the map on which to transmit the data message to the destination node.

35. A computer system as in claim 34, wherein establishing a virtual network connection includes establishing a virtual private network connection between the receiving node and sending node based on IKE (Internet Key Exchange) protocol and Ipsec (Internet Protocol Security).

36. A computer system as in claim 33 that further performs operations of:

in response to identifying that the destination address of the data message matches network address information in the map, identifying whether a corresponding virtual network connection specified in the map has been established and, if so, transmitting the data message on the established virtual network connection to the destination node.

37. A computer system as in claim 31, wherein the network address information identifies a single host computer.

38. A computer system as in claim 31, wherein the network address information identifies a range of host computers that are part of a network coupled to the first node.

39. A computer system as in claim 31, wherein the corresponding gateway identifier is a network address of the at least one host computer.

40. A computer system as in claim 31, wherein the gateway is located in the sending node.

41. A computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, enable the processing device to perform the steps of:

receiving i) network address information associated with at least one host computer, and ii) a corresponding gateway identifier of a gateway in the physical network;

generating a notification message including the network address information and the corresponding gateway identifier; and

transmitting the notification message to a second node of the physical network enabling the second node to establish a virtual network

connection between the second node and the first node on which to forward data messages to the at least one host computer based on the corresponding gateway identifier.

42. A computer system at a first node of a physical network that at least partially supports a virtual network connection, the computer system comprising:

means for receiving i) network address information associated with at least one host computer, and ii) a corresponding gateway identifier of a gateway in the physical network;

means for generating a notification message including the network address information and the corresponding gateway identifier; and

means for transmitting the notification message to a second node of the physical network enabling the second node to establish a virtual network connection between the second node and the first node on which to forward data messages to the at least one host computer based on the corresponding gateway identifier.

43. A computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, enable the processing device to perform the steps of:

receiving a notification message from a sending node of the physical network, the notification message including network address information and a corresponding gateway identifier of a gateway of the physical network; and

based on contents of the notification message, modifying a map at the receiving node to include the network address information and configuration data identifying at least part of a virtual network connection between the receiving node and the sending node on which to forward data messages through the gateway to a destination node.

44. A computer system at a receiving node of a physical network that at least partially supports a virtual network connection, the computer system comprising:

means for receiving a notification message from a sending node of the physical network, the notification message including network address information and a corresponding gateway identifier of a gateway of the physical network; and

means for modifying a map at the receiving node to include the network address information and configuration data identifying at least part of a virtual network connection between the receiving node and the sending node on which to forward data messages through the gateway to a destination node.

45. In a physical network supporting virtual private network connections terminating at customer edge routers coupled to a service provider network, a method comprising:

at a first customer edge router:

receiving a range of network addresses associated with host computers coupled to the first customer edge router;

in addition to receiving the range of network addresses, receiving a security gateway identifier associated with a second customer edge router of the service provider network;

generating and transmitting a notification message including the range of network addresses and the security gateway identifier to the second customer edge router; and

at the second customer edge router:

receiving the notification message;

based on contents of the notification message, generating a map to include the range of network addresses and a corresponding

virtual private network connection between the second customer edge router and first customer edge router; and

prior to forwarding data messages through the second customer edge router to a computer having a network address in the range of network addresses, utilizing the map to identify on which virtual private network to forward the data messages.